

**Appl. No. 10/716,588  
Amdt. dated August 6, 2007  
Reply to Office Action of June 4, 2007**

**Listing of Claims:**

1. (Presently Presented) A method, comprising:  
calculating a first part of a message authentication function by a first processor;  
calculating a second part of the message authentication function by a second processor;  
combining the results of the first and second parts into a message authentication code by the first or second processors; and  
using the message authentication code to authenticate data.
2. (Presently Presented) The method of claim 1 wherein the message authentication code is used, in part, to authenticate data transmitted between the first processor and a third processor.
3. (Original) The method of claim 1 wherein the first and second processors are provided in separate computer systems.
4. (Original) The method of claim 1 wherein the first and second parts of the message authentication function consist of one-way hash functions.
5. (Original) The method of claim 1 wherein calculating the first part comprises calculating a value without having a data key associated with the function.
6. (Original) The method of claim 1 wherein calculating the second part comprises calculating a value for a data set without having contents of the data set.
7. (Presently Presented) The method of claim 6 further comprising storing the contents into a non-volatile memory coupled to the first processor and storing the message authentication code into non-volatile memory coupled to the second processor.

**Appl. No. 10/716,588  
Amdt. dated August 6, 2007  
Reply to Office Action of June 4, 2007**

8. (Presently Presented) The method of claim 1 further comprising calculating the message authentication code using the message authentication function on a data set, wherein the message authentication code can be used to authenticate a record that consists of the data set.

9. (Presently Presented) A method implemented in a first computer, comprising:

- creating a record;
- computing a first part of a message authentication function using contents of the record;
- providing the result of the first part to a second computer, and
- receiving the result of a second part of the message authentication function from the second computer, said second part computed using a data key that is not available to the first computer.

10. (Original) The method of claim 9 further comprising encrypting the record and transmitting the record to a third computer.

11. (Presently Presented) A system, comprising:

- a first processor configured to compute a first part of a multi-part message authentication function;
- a second processor in communication with the first processor, the second processor is configured to compute a second part of the message authentication function;

wherein the first part of the message authentication function is based on the contents of a record and the second part is based on a data key, wherein the data key is inaccessible by the first processor and the record contents are inaccessible by the second processor.

**Appl. No. 10/716,588  
Amdt. dated August 6, 2007  
Reply to Office Action of June 4, 2007**

12. (Original) The system of claim 11 wherein the message authentication function is used to authenticate data transmitted between the first processor and a third processor.

13. (Presently Presented) The system of claim 11 wherein the second processor combines the message authentication function parts and provides the combined message authentication function result to the first processor to permit the first processor to authenticate the record with the combined message authentication function result and provide the authenticated record to a third processor.

14. (Original) The system of claim 11 wherein the first processor receives the second part from the second processor and encodes a record with the second part and transmits the encoded record to a third processor.

15. (Presently Presented) The system of claim 11 wherein the first processor receives the record from a third processor, computes the first part of the message authentication function using contents of the record, and sends the result of the first part of the message authentication function and a message authentication code in the record to the second processor.

16. (Presently Presented) The system of claim 11 wherein the second processor combines the message authentication function parts validates a message authentication code using the combined message authentication function result.

17. (Presently Presented) A computer, comprising:  
a processor; and  
memory containing code executable by said processor;  
wherein said executable code causes said processor to compute a first part of a message authentication function based on contents of a

**Appl. No. 10/716,588  
Amdt. dated August 6, 2007  
Reply to Office Action of June 4, 2007**

record, to provide the result of said first part to a second computer, to receive a result of a second part of the message authentication function from the second computer, and to encode the record with the result of the second part; and

wherein the record contents are hidden from the second computer and wherein the second part is computed by the second computer using a data key that is hidden from the first computer.

18. (Cancelled).

19. (Previously Presented) A system, comprising:

a server;

a client coupled to the server; and

a witness computer coupled to the client;

wherein the client has access to data that is inaccessible to the witness computer and wherein the witness computer has access to a data key that is inaccessible to the client, and

wherein at least some communications between the server and the client are authenticated by combining a multi-part message authentication function, a first part of the message authentication function being computed by the client using the data and a second part of the message authentication function being computed by the witness computer using the data key.

20. (Previously Presented) The system of claim 19, wherein the multi-part message authentication function is a decomposable hashed-based message authentication code (HMAC).